(19) JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: **08242488 A**
(43) Date of publication of application: **17.09.1996**

(51) Int. Cl **H04Q 7/38**
G09C 1/00, H04L 9/00, H04L 9/10, H04L 9/12

(21) Application number: **07043129**
(22) Date of filing: **02.03.1995**

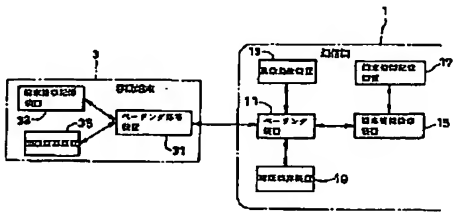
(71) Applicant: **N T T IDO TSUSHINMO KK**
(72) Inventor: **HAGIWARA JUNICHIRO**
YAMAGATA KATSUHIKO

(54) MOBILE COMMUNICATION SYSTEM

(57) Abstract:

PURPOSE: To instantaneously complete the authentication after the paging by performing simultaneously these authentication and paging, to release the radio resources, and to attain the effective management of the radio resources.

CONSTITUTION: In a paging state of a mobile terminal 3, a paging device 11 sends the random numbers of a random number generation device 13 to the terminal 3 together with a paging signal. The terminal 3 extracts a random number, and a paging answer device 31 calculates the authentication information received from a terminal information storage 33 and the extracted random number through an authentication arithmetic unit 35. Then the device 31 adds the arithmetic result into paging answer signal to send them to a communication network 1 and extracts the authentication arithmetic result. At the same time, the device 11 sends the authentication information obtained from a terminal information storage 17 to an authentication arithmetic unit 19 together with the random number via a terminal information retrieval device 15 to obtain again the authentication arithmetic result. This arithmetic result is compared with the extracted authentication arithmetic result for decision of the correctness of the terminal 3. Thereby, the reserved radio resources can be instantaneously released after the paging and before the transmission/reception of various signals when a wrong mobile terminal receives an incoming call.



(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（A）**　(11)特許出願公開番号

特開平8－242488

(43)公開日　平成８年(1996)９月17日

(51)Int.Cl.[6]		識別記号	庁内整理番号	ＦＩ			技術表示箇所
Ｈ０４Ｑ	7/38			Ｈ０４Ｂ	7/26	１０９Ｒ	
Ｇ０９Ｃ	1/00		7259－5Ｊ	Ｇ０９Ｃ	1/00		
Ｈ０４Ｌ	9/00			Ｈ０４Ｌ	9/00	Ｚ	
	9/10						
	9/12						

審査請求　未請求　請求項の数２　ＯＬ　（全 ７ 頁）

(21)出願番号　特願平7－43129

(22)出願日　平成７年(1995)３月２日

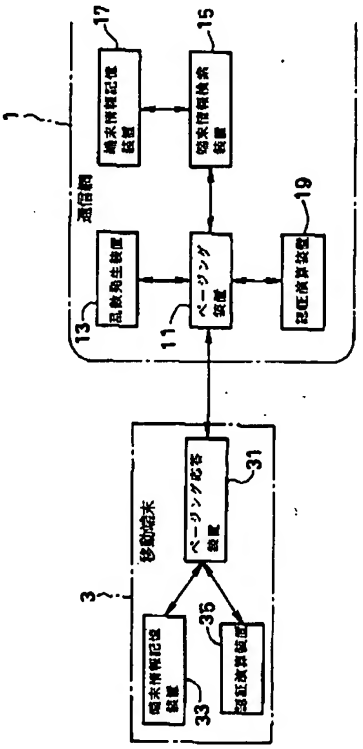
(71)出願人　392026693
エヌ・ティ・ティ移動通信網株式会社
東京都港区虎ノ門二丁目10番１号
(72)発明者　萩原　淳一郎
東京都港区虎ノ門二丁目10番１号　エヌ・ティ・テイ移動通信網株式会社内
(72)発明者　山縣　克彦
東京都港区虎ノ門二丁目10番１号　エヌ・ティ・テイ移動通信網株式会社内
(74)代理人　弁理士　三好　秀和　（外３名）

(54)【発明の名称】　移動通信方式

(57)【要約】

【目的】　本発明は、限りある無線資源の使用効率を改善し、効率の良い無線資源管理を行い得る移動通信方式を提供することを目的とする。

【構成】　網は、ページング信号中に移動端末の認証のための乱数を含めて移動端末に送出し、移動端末では、このページング信号中の乱数と認証情報との第１の認証演算結果をページング応答信号に含めて網に送出し、さらに網では、このページング応答信号中の第１の認証演算結果を網内で生成した第２の認証演算結果と比較することにより応答移動端末の正当性を判断することを要旨とする。



1

【特許請求の範囲】

【請求項１】　網は、ページング信号中に移動端末の認証のための乱数を含めて移動端末に送出し、移動端末では、このページング信号中の乱数と認証情報との第１の認証演算結果をページング応答信号に含めて網に送出し、さらに網では、このページング応答信号中の第１の認証演算結果を網内で生成した第２の認証演算結果と比較することにより応答移動端末の正当性を判断することを特徴とする移動通信方式。

【請求項２】　網内に、移動端末の認証のための乱数を発生する乱数発生手段と、端末毎の認証情報を記憶する網内記憶手段と、この網内記憶手段に記憶される認証情報と前記乱数発生手段で発生された乱数とを用いて認証演算を行い第２の認証演算結果を得る網内演算手段と、ページング信号中に前記乱数発生手段で発生された乱数を含めて送出し、移動端末からのページング応答信号中の第１の認証演算結果を前記第２の認証演算結果と比較することにより応答移動端末の正当性を判断するページング手段とを備え、

移動端末内に、自端末の認証情報を記憶する端末内記憶手段と、この端末内記憶手段に記憶される当該端末の認証情報とページング信号中の乱数とを用いて認証演算を行う端末内演算手段と、網からのページング信号中の識別情報と自端末の識別情報が一致したときに、このページング信号中の乱数を用いて前記端末内演算手段が認証演算を行い得られた第１の認証演算結果をページング応答信号に含めて網に送出するページング応答手段とを有することを特徴とする移動通信方式。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】本発明は、ページングシステムを利用する移動通信方式に関するものである。

【０００２】

【従来の技術】一般に、移動通信において着信がある場合、移動する着端末の位置を特定するためページングを行う。つまり特定の位置登録エリアにおいて、着端末を識別する情報を情報要素に持つ信号を網から一斉報知し、この一斉報知された情報が自分の識別情報であると判断した移動端末のみが、応答信号を網に返し、当該移動端末自身の位置を報告する。

【０００３】一方、網は、この応答した移動端末の正当性を調べるために、具体的には正当な利用者であることを識別し不正使用の防止を計るために、移動端末に対して認証要求信号を送信する。この認証要求信号を受け取った移動端末は当該移動端末自身の持つ認証情報を用いて応答を作成し、認証応答信号を網に返す。網ではこの認証応答信号の内容を網自身の期待する内容と比較することにより、この移動端末の正当性を判断する。もし、ここで例えば認証応答機能がない、正当な認証情報を持たないために網によって期待される認証応答を生成する

2

能力がない等により、当該移動端末が不正のものならば認証が正しく完了しないのでそれ以降、網へのアクセスが規制される。一方、移動端末が正当のものならば認証が正しく完了し、網へのアクセスが進展してゆく。

【０００４】以下、図３を参照して、上述した認証手順を秘密鍵暗号アルゴリズムを用いた場合を例に具体的に説明する。

【０００５】まず、網内の乱数発生装置１１３で生成された認証用の乱数は、送受信装置と比較器からなる送受信・比較装置１１１によって着端末としての移動端末１０３に送られ、この移動端末１０３において送受信装置１３１で受信される。送受信装置１３１は、これと秘密鍵記憶装置１３３から得られた秘密鍵を認証演算装置１３５に送る。認証演算装置１３５は認証演算結果を出力し、送受信装置１３１を介して通信網１０１に送る。

【０００６】網１０１においては、移動端末１０３からの認証演算結果を送受信・比較装置１１１を介して受信する。送受信・比較装置１１１は秘密鍵検索装置１１５に当該移動端末１０３の秘密鍵の取得を依頼する。秘密鍵検索装置１１５は秘密鍵記憶装置１１７より得た秘密鍵を送受信・比較装置１１１に送る。送受信・比較装置１１１はこの秘密鍵を先に乱数発生装置１１３で生成された認証用の乱数と共に認証演算装置１１９に送る。認証演算装置１１９は認証演算結果を送受信・比較装置１１１に送る。送受信・比較装置１１１はこの認証演算結果と、当該移動端末１０３から得られた認証演算結果を比較する。ここで２つの認証演算結果が一致していたら認証可であり、一致していなければ認証不可である。

【０００７】次に、着信の際の通信手順の一例として日本標準の移動通信規格ＰＨＳ（Personal Handy-phone System）（公衆用）における手続きを図４に示す。

【０００８】図４に示すように、まず、通信網１０１は移動端末１０３に対してページング要求（ステップＳ１０１）を行う。次に、当該移動端末１０３はリンクチャネル確立要求（ステップＳ１０３）を行い、リンクチャネル割当（ステップＳ１０５）が成される。以下、順次ページング応答（ステップＳ１０７）の後に、ステップＳ１０９で所定の信号送受（ＳＥＴＵＰ、ＣＡＬＬＰＲＯＣ、定義情報要求、定義情報応答、ＲＴ機能要求、ＲＴ機能要求応答、秘匿鍵設定、ＭＭ機能要求、ＭＭ機能要求応答）が行われる。そして、さらに認証乱数を含む認証要求（ステップＳ１１１）及び認証演算結果を含む認証応答（ステップＳ１１３）により認証が行われる。

【０００９】従って、もし不正移動端末がページングに対して応答した場合、いずれ無線資源を解放しなければならないのにも拘らず、認証が終わるまでの信号送受の間、無駄に無線資源を保留していることになる。

【００１０】

【発明が解決しようとする課題】上述したように、従来の移動通信方式では着信の際に、認証が完了するまでの

間は無線資源を保留しておかなければならず、そのため無線資源の使用効率が良くない。

【0011】本発明は、上記課題に鑑みてなされたもので、限りある無線資源の使用効率を改善し、効率の良い無線資源管理を行い得る移動通信方式を提供することを目的とする。

【0012】

【課題を解決するための手段】上記目的を達成するため本願第1の発明は、網は、ページング信号中に移動端末の認証のための乱数を含めて移動端末に送出し、移動端末では、このページング信号中の乱数と認証情報との第1の認証演算結果をページング応答信号に含めて網に送出し、さらに網では、このページング応答信号中の第1の認証演算結果を網内で生成した第2の認証演算結果と比較することにより応答移動端末の正当性を判断することを要旨とする。

【0013】また、本願第2の発明は、網内に、移動端末の認証のための乱数を発生する乱数発生手段と、端末毎の認証情報を記憶する網内記憶手段と、この網内記憶手段に記憶される認証情報と前記乱数発生手段で発生された乱数とを用いて認証演算を行い第2の認証演算結果を得る網内演算手段と、ページング信号中に前記乱数発生手段で発生された乱数を含めて送出し、移動端末からのページング応答信号中の第1の認証演算結果を前記第2の認証演算結果と比較することにより応答移動端末の正当性を判断するページング手段とを備え、移動端末内に、自端末の認証情報を記憶する端末内記憶手段と、この端末内記憶手段に記憶される当該端末の認証情報とページング信号中の乱数とを用いて認証演算を行う端末内演算手段と、網からのページング信号中の識別情報と自端末の識別情報が一致したときに、このページング信号中の乱数を用いて前記端末内演算手段が認証演算を行い得られた第1の認証演算結果をページング応答信号に含めて網に送出するページング応答手段とを有することを要旨とする。

【0014】

【作用】本願第1の発明の移動通信方式は、網は、まずページング信号中に移動端末の認証のための乱数を含めて移動端末に送出し、移動端末では、このページング信号中の乱数と当該移動端末の認証情報との認証演算を行い、この演算結果を第1の認証演算結果としてページング応答信号に含めて網に送出する。さらに網では、このページング応答信号中の第1の認証演算結果を網内で生成した第2の認証演算結果と比較することで、ページングと同時に当該応答移動端末の正当性を判断する。

【0015】本願第2の発明の移動通信方式は、網内のページング手段は、まずページング信号中に前記乱数発生手段で発生された乱数を含め、当該ページング信号を移動端末へ送出する。

【0016】このページング信号を受信した移動端末の

端末内演算手段は、端末内記憶手段に記憶される当該自端末の認証情報と網からのページング信号中の乱数とを用いて認証演算を行う。

【0017】移動端末内のページング応答手段は、網からのページング信号中の識別情報と自端末の識別情報が一致したときに、このページング信号中の乱数を用いて前記端末内演算手段が認証演算を行い得られた第1の認証演算結果をページング応答信号に含めて網に送出する。

【0018】網内の網内演算手段は、網内記憶手段に記憶される端末毎の認証情報と前記乱数発生手段で発生された認証のための乱数とを用いて認証演算を行い第2の認証演算結果を得る。さらに網内のページング手段は、移動端末からのページング応答信号中の第1の認証演算結果を前記第2の認証演算結果と比較することにより応答移動端末の正当性を判断する。これにより、ページングと同時に当該移動端末の正当性が判断される。

【0019】

【実施例】以下、本発明に係る一実施例を図面を参照して説明する。図1は本発明に係る移動通信方式の構成を示したブロック図である。

【0020】図1に示すように、通信網1は、ページング装置11と、このページング装置11と接続される乱数発生装置13、端末情報検索装置15、認証演算装置19及びこの認証演算装置19と接続される端末情報記憶装置17によって構成される。また、移動端末3は、通信網1のページング装置11と無線回線を介して接続されるページング応答装置31と、このページング応答装置31と接続される端末情報記憶装置33及び認証演算装置35によって構成される。

【0021】次に、図1を参照して、本実施例の作用を認証手順に沿って具体的に説明する。まず、移動端末3のページングに際して、通信網1内のページング装置11は乱数発生装置13で発生された乱数を得て、この乱数をページング信号中に含めて着移動端末3に向けて送出する。

【0022】移動端末3では、まずページング信号を受信してページング信号中の乱数を抽出し、ページング応答装置31が端末情報記憶装置33から得た認証情報とこの抽出したページング信号中の乱数とを認証演算装置35に送り、さらに認証演算装置35で得た第1の認証演算結果としての認証演算結果をページング応答信号に含めて通信網1に送出する。

【0023】通信網1ではページング応答信号を受信し、ページング応答信号に含まれる認証演算結果を抽出する。一方、ページング装置11は、端末情報検索装置15に当該移動端末の認証情報の取得を依頼し、端末情報検索装置15が端末情報記憶装置17より得た認証情報を当該乱数とともに認証演算装置19に送って得た第2の認証演算結果としての認証演算結果を前記抽出され

5

た第１の認証演算結果としての認証演算結果と比較することにより当該移動端末３の正当性を判断する。

【００２４】次に、図２を参照して、本発明の方法を適用したＰＨＳ（公衆用）の着信手順の一例を説明する。この図２では図４と異なりページングと認証を同時に行う。すなわち、まず、ステップＳ１で通信網１から移動端末３に対してページング要求を行う。このページング要求に対して移動端末３は、ステップＳ３でページング応答を行う。このページングの後に、ステップＳ５で所定の信号送受（リンクチャネル確立要求（ステップＳ５１）、リンクチャネル割当（ステップＳ５３）、ＳＥＴＵＰ、ＣＡＬＬＰＲＯＣ、定義情報要求、定義情報応答、ＲＴ機能要求、ＲＴ機能要求応答、秘匿鍵設定、ＭＭ機能要求、ＭＭ機能要求応答（ステップＳ５５））が行われる様になっている。

【００２５】従って、もし不正移動端末への着信があった場合、様々な信号送受を待たずに、ページング後即座に保留していた無線資源を解放することができる。

【００２６】尚、上記の実施例では本発明をＰＨＳに適用した場合を例にとって説明したが、本発明はこれに限定されること無く、例えばセルラ通信、ページャ（いわゆるポケベル）等の適宜のページング方式の移動通信方式に適用することができる。

【００２７】

6

【発明の効果】以上説明したように本発明は、ページングと認証を同時に行うことから、ページング後即座に認証が完了し、無線資源の解放判断ができる。この結果効率のよい無線資源管理が可能となる等の効果を奏する。

【図面の簡単な説明】

【図１】本発明に係る一実施例の構成を示すブロック図である。

【図２】本発明の方法を適用したＰＨＳ（公衆用）の着信通信手順の一例を示す図である。

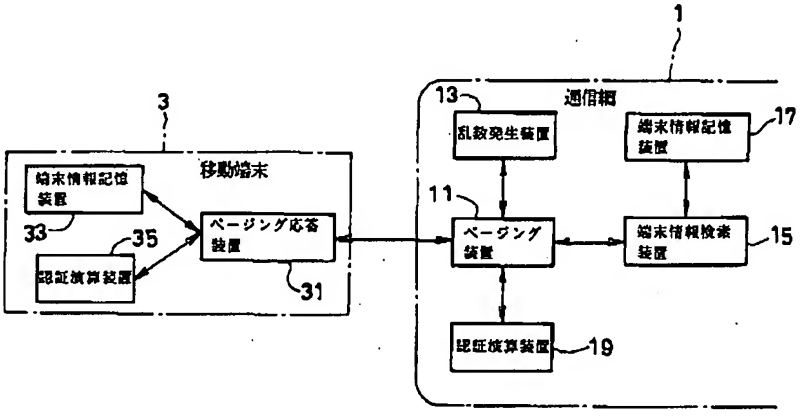
【図３】秘密鍵暗号アルゴリズムを用いた認証を実施する場合の構成を示すブロック図である。

【図４】ＰＨＳ（公衆用）の着信通信手順の一例を示す図である。

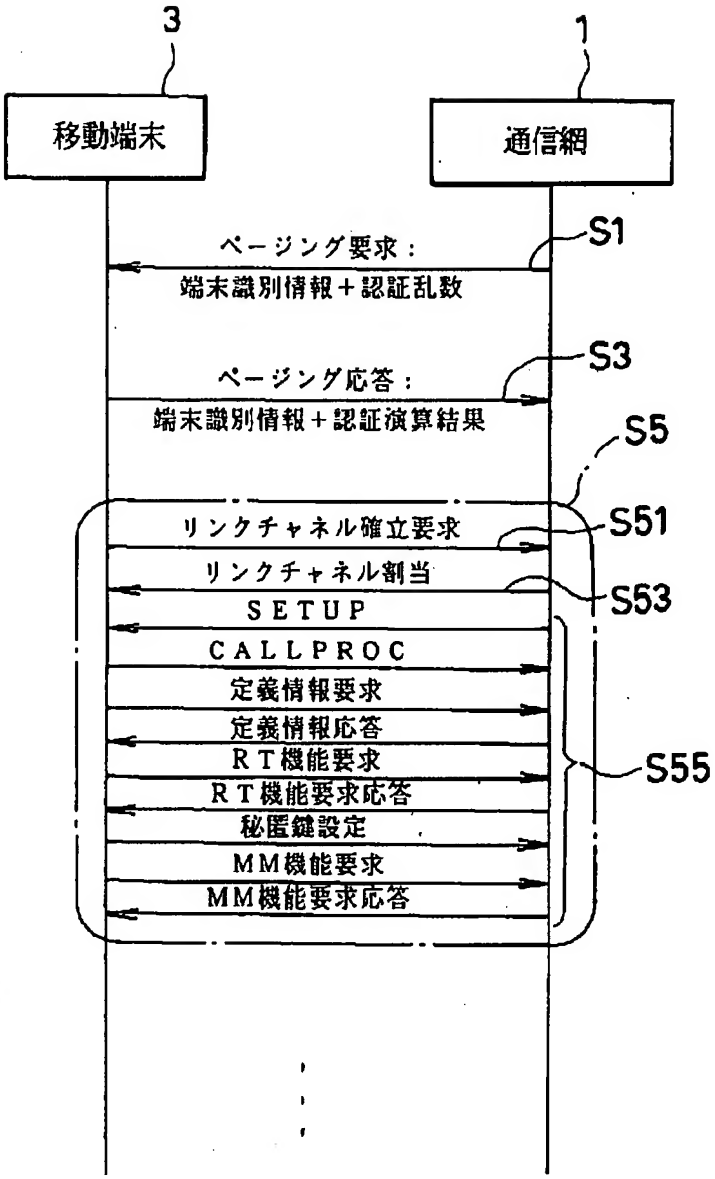
【符号の説明】

１　通信網
３　移動端末
１１　ページング装置
１３　乱数発生装置
１５　端末情報検索装置
１７，３３　端末情報記憶装置
１９　認証演算装置
３１　ページング応答装置
３５　認証演算装置

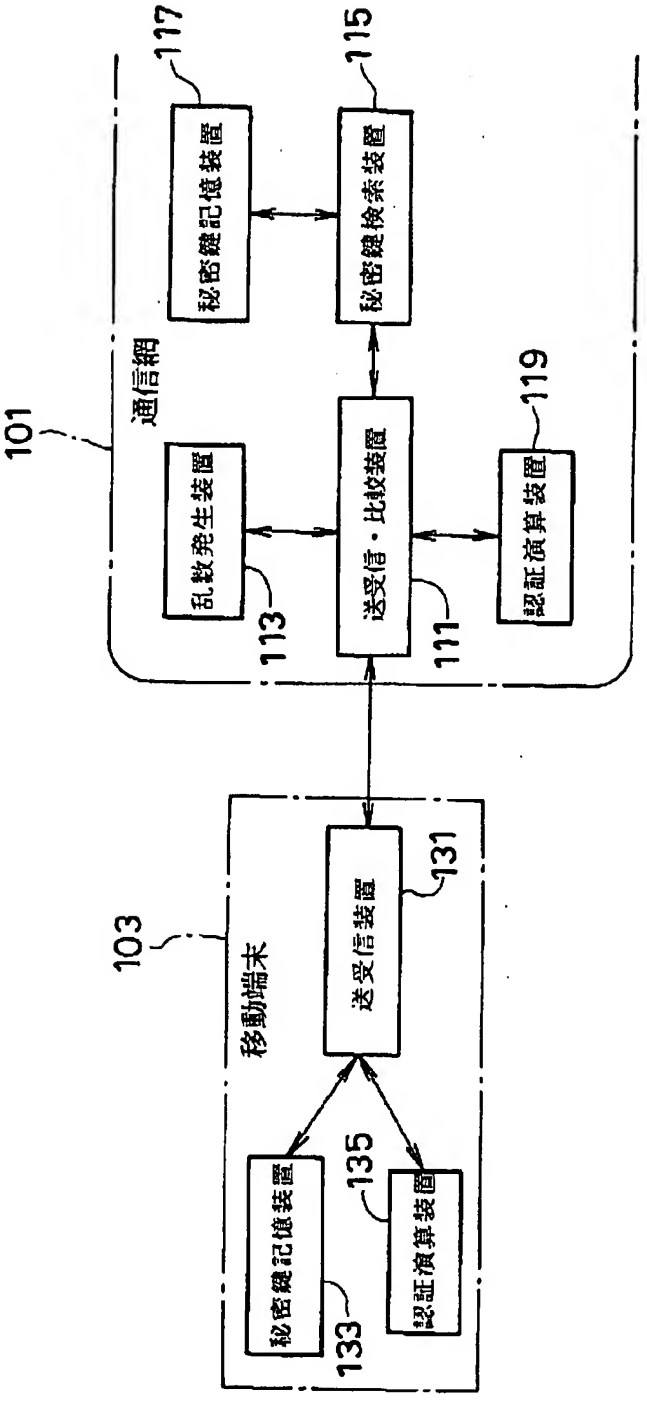
【図１】



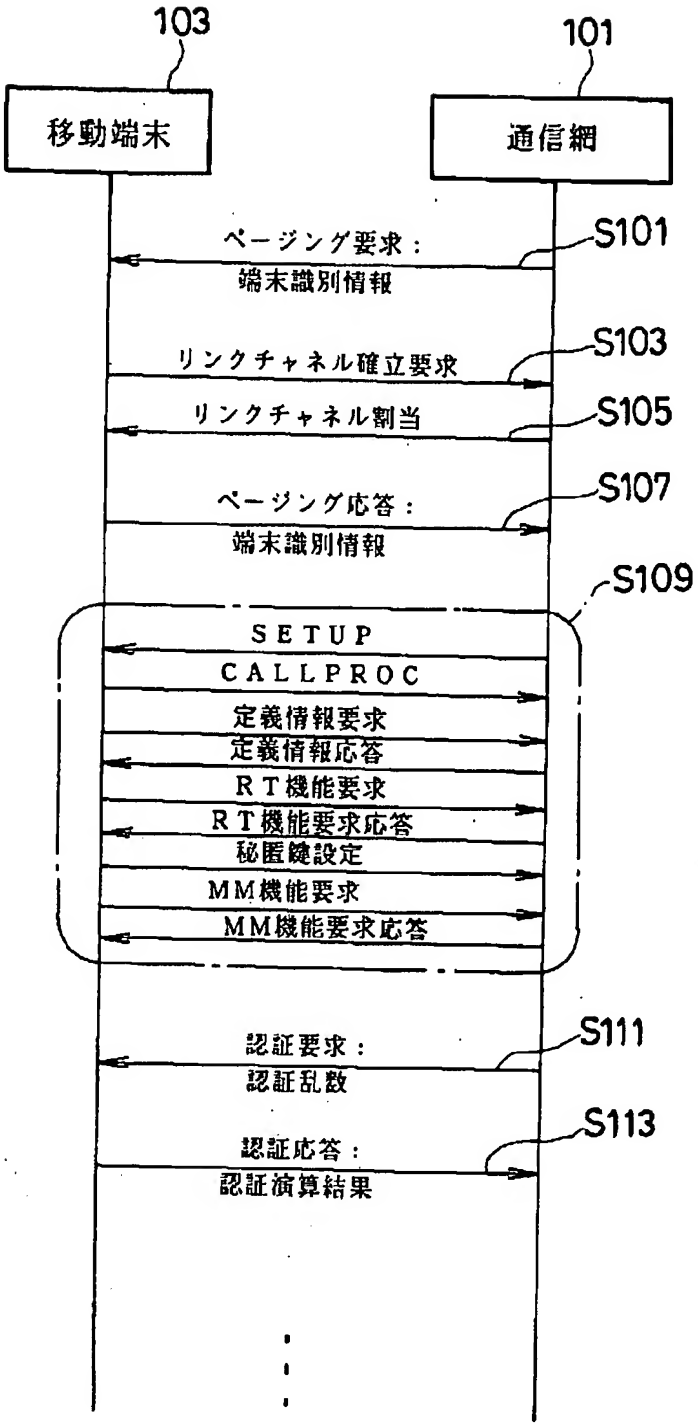
【図2】


3
1
移動端末
通信網
ページング要求：
端末識別情報＋認証乱数
S1
ページング応答：
端末識別情報＋認証演算結果
S3
S5
リンクチャネル確立要求
S51
リンクチャネル割当
S53
SETUP
CALLPROC
定義情報要求
定義情報応答
RT機能要求
RT機能要求応答
秘匿鍵設定
MM機能要求
MM機能要求応答
S55

【図3】


101
通信網
117
秘密鍵記憶装置
115
秘密鍵検索装置
乱数発生装置
113
送受信・比較装置
111
認証演算装置
119
103
移動端末
送受信装置
131
秘密鍵記憶装置
133
135
認証演算装置

【図4】


103
101
移動端末
通信網
ページング要求：
端末識別情報
S101
リンクチャネル確立要求
S103
リンクチャネル割当
S105
ページング応答：
端末識別情報
S107
S109
SETUP
CALLPROC
定義情報要求
定義情報応答
RT機能要求
RT機能要求応答
秘匿鍵設定
MM機能要求
MM機能要求応答
認証要求：
認証乱数
S111
認証応答：
認証演算結果
S113